

What is Claimed is:

1. An encryption device comprising XOR means and  
nonlinear transform means, said encryption device  
5 further comprising:

random number generator means for generating a  
random number;

q fixed values, where q is an integer; and

10 a first selector for selecting one of said q fixed  
values in response to the random number;

said XOR means XORing an input thereto with an XOR  
of a key with said selected fixed value.

15 2. The encryption device according to claim 1, further  
comprising:

q sets of masked fixed tables; and

a second selector for selecting one of said q sets  
of fixed tables in response to the random number,

20 said nonlinear transform means nonlinearly  
transforming an input thereto in accordance with the  
selected set of fixed tables.

3. The encryption device according to claim 1, further  
comprising:

25 an encrypting unit comprising said first XOR means  
and said nonlinear transform means;

second XOR means for XORing an input to said  
encryption device with a fixed value selected in response  
to the random number; and

30 third XOR means for XORing an output from said  
encrypting unit with the fixed value selected in response  
to the random number.

35 4. An encryption device comprising XOR means and  
nonlinear transform means, said encryption device  
further comprising:

random number generator means for generating a

random number;

q sets of masked fixed tables, where q is an integer;  
and

a selector for selecting one of said q sets of fixed  
5 tables in response to the random number,  
said nonlinear transform means nonlinearly  
transforming an input thereto in accordance with said  
selected set of fixed tables.

10 5. The encryption device according to claim 4, further  
comprising a plurality of encrypting rounds, wherein  
each of said plurality of encrypting rounds  
comprises the XOR means, the fixed tables and the selector,  
for that round; and

15 the fixed tables for said plurality of respective  
encrypting rounds are identical.

6. The encryption device according to claim 4, wherein  
an equation,  $(c_{0,j} \text{ XOR } c_{1,j}) \vee (c_{1,j} \text{ XOR } c_{2,j}) \vee \dots \vee (c_{q-2,j}$   
20  $\text{ XOR } c_{q-2,j}) = (11111111)_2$ , is satisfied, where a fixed table  
before masking is defined as  $S[x]$ , and a j-th masked table  
is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  ( $j = 0, 1, \dots, 15$ ).

7. The encryption device according to claim 4, wherein  
25 the number of sets of tables is  $q = 2$ , and an equation,  
 $c_{0,j} \text{ XOR } c_{1,j} = (10101010)_2$  or  $(01010101)_2$ , is satisfied,  
where a fixed table before masking is defined as  $S[x]$ ,  
and a j-th masked table is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$   
( $j = 0, 1, \dots, 15$ ).

30 8. The encryption device according to claim 4, wherein  
an equation,  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j}$   
 $\text{ XOR } d_{q-2,j}) = (11111111)_2$ , is satisfied, where a fixed table  
before masking is defined as  $S[x]$ , and a j-th masked table  
35 is defined as  $S_j[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  ( $j = 0, 1, \dots, 15$ ).

9. The encryption device according to claim 4, said

nonlinear transform means being Subbyte means;

said encryption device further comprising means for shifting an input, and means for mixedcolumning an input.

5 10. An encryption device comprising:

random number generator means for generating a random number;

a plurality of encrypting units coupled in parallel; and

10 a selector for selecting one of said plurality of encrypting units in response to the random number;

each of said plurality of encrypting units comprises XOR means and nonlinear transform means.

15 11. The encryption device according to claim 10, wherein said XOR means of said selected encrypting unit XORs an input thereto with an XOR of a key with a fixed value.

12. The encryption device according to claim 10, wherein  
20 said nonlinear transform means nonlinearly transforms an input thereto in accordance with a fixed table.

13. The encryption device according to claim 10, wherein  
25 each of said plurality of encrypting units comprises:

second XOR means for XORing an input thereto into that encrypting unit with a fixed value; and

30 third XOR means for producing an XOR of an input with a fixed value as an output from that encrypting unit.

14. The encryption device according to claim 10, wherein  
said nonlinear transform means of said selected encrypting unit nonlinearly transforms an input thereto  
35 in accordance with a fixed table.

15. The encryption device according to claim 10, wherein

each of said plurality of encrypting units comprises a plurality of encrypting rounds;

each of said plurality of encrypting rounds comprises XOR means for XORing an input thereto with an XOR of a key with a fixed value, and nonlinear transform means for nonlinearly transforming an input thereto in accordance with a fixed table.

16. An encryption device comprising random number generator means for generating a random number and a first plurality of encrypting rounds, wherein

each of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q fixed values, where q is an integer;

a selector for selecting one of said q fixed values in response to the random number; and

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value.

17. The encryption device according to claim 16, wherein said nonlinear transform means further comprises therein a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table; and a selector for selecting one of said plurality of nonlinear transform means.

18. The encryption device according to claim 17, wherein the fixed tables of said respective nonlinear transform means in said respective encrypting rounds are identical.

19. The encryption device according to claim 16, wherein

a mask is canceled over subsequent ones of said plurality of encrypting rounds.

20. The encryption device according to claim 16, wherein  
5       masking is performed in each of a second plurality of encrypting rounds of said first plurality of encrypting rounds, said second plurality being smaller than said first plurality.

10 21. An encryption device comprising a random number generator means for generating a random number, and a plurality of encrypting rounds, wherein

each of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly  
15 transforming an input thereto; and XOR means for XORing a first input thereto and a second input thereto;

the second input to said XOR means is connected to an output of said nonlinear transform means; and

said nonlinear transform means comprises therein  
20 nonlinear transform means for nonlinearly transforming an input thereto in accordance with a fixed table and in accordance with the random number.

22. An encryption device, comprising:

25       random number generator means for generating a random number;

a plurality of encrypting units coupled in parallel; and

a selector for selecting one of said plurality of  
30 encrypting units in response to the random number, wherein,

each of said encrypting units comprises a plurality of encrypting rounds;

each of said encrypting rounds comprises:

35       nonlinear transform means for nonlinearly transforming an input thereto; and

XOR means for XORing a first input thereto with a

second input thereto; and

the second input to said XOR means is coupled to an output of said nonlinear transform means.

- 5 23. The encryption device according to claim 22, wherein said nonlinear transform means comprises:

further XOR means for XORing an input thereto with an XOR of a key with a fixed value; and

10 further nonlinear transform means for nonlinearly transforming an input thereto in accordance with a fixed table.

24. The encryption device according to claim 22, wherein an equation,  $(d_{0,j} \text{ XOR } d_{1,j}) \vee (d_{1,j} \text{ XOR } d_{2,j}) \vee \dots \vee (d_{q-2,j} \text{ XOR } d_{q-1,j}) = (1111)_2$ , is satisfied, where a fixed table before masking is defined as  $S_j[x]$ , and a  $j$ -th masked table is defined as  $S_j'[x \text{ XOR } c_{i,j}] \text{ XOR } d_{i,j}$  ( $j = 0, 1, \dots, 7$ ).

25. A program stored on a storage medium for use in an encryption device, said program operable to effect the steps of:

selecting one of  $q$  fixed values, where  $q$  is an integer, in response to a random number;

25 XORing an input value with an XOR of a key with said selected fixed value;

selecting one set of  $q$  sets of masked fixed tables in response to the random number; and

30 nonlinearly transforming an input value in accordance with said selected set of fixed tables.

26. A program stored on a storage medium for use in an encryption device, said program operable to effect the steps of:

35 selecting one of a plurality of encryption processes in response to a random number, and

encrypting an input value in accordance with said selected encryption process to provide an output;

the encrypting step comprising the steps of:  
XORing an input value with an XOR of a key with a  
fixed value, and  
nonlinear transforming an input value in accordance  
5 with a set of fixed tables.

27. A program stored on a storage medium for use in an  
encryption device, said program operable to effect the  
steps of:

10 nonlinear transforming an input value to provide an  
output, and

XORing a first input value with said output as a  
second input value;

the nonlinear transforming step comprising the steps  
15 of:

selecting one of q fixed values in response to a  
random number, where q is an integer,

XORing an input value with an XOR of a key with said  
selected fixed value, and

20 nonlinear transforming an input value in accordance  
with a set of fixed tables associated with the random  
number.

28. A program stored on a storage medium for use in an  
25 encryption device, said program operable to effect the  
steps of:

selecting one of a plurality of encryption processes  
in response to a random number, and

30 encrypting an input value in accordance with said  
selected encryption processes to provide an output;

the encrypting step comprising the steps of:

nonlinear transforming an input value to produce an  
output, and

35 XORing a first input value with said output as a  
second input value.